UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

TRACEY DAMRAU and DANIELLE OSHEA, individually and on behalf of all others similarly situated, Plaintiffs, v. COLIBRI GROUP, INC., Defendant.	Civil Action No. 4:24-cv-1441 **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Tracey Damrau ("Plaintiff Damrau") and Danielle Oshea ("Plaintiff Oshea"), individually and on behalf of all others similarly situated, make the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to themselves or their counsel, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiffs bring this action to redress Defendant Colibri Group, Inc.'s ("Colibri") practices of selling, renting, transmitting, and/or otherwise disclosing, to various third parties, records containing the personal information (including names and addresses) of each of their customers, along with detailed information revealing the subscription to prerecorded video content or titles and subject matter of

prerecorded video and other audiovisual materials requested or obtained by each customer in violation of the Video Privacy Protection Act, 18 U.S.C. §2710 et seq. ("VPPA").

2. Over the past two years, Defendant has systematically transmitted (and continues to transmit today) its customers' personally identifying video viewing information to third parties, such as Meta Platforms, Inc. ("Meta") and TikTok Inc. ("Tiktok"). The programming code for Meta is called the "Meta Pixel," which Defendant chose to install on the websites of its portfolio of companies and brands, including but not limited to the www.elitelearning.com website, the www.homeceuconnection.com, the www.colibrirealestate.com website, the www.mckissock.com website, and the www.fhea.com website (the "Websites"). The programming code for TikTok is called the "TikTok Pixel," which Defendant chose to install on the Websites of its Colibri Group portfolio of companies and brands.

3. Each of Defendant's Websites operate in the same manner as alleged in more detail below.

4. The information Defendant disclosed (and continues to disclose) to Meta via the Meta Pixel includes the customer's Facebook ID ("FID") and the subscription to access prerecorded videos or the specific title of prerecorded videos that each of its customers purchased on any one of its Websites. An FID is a unique

sequence of numbers linked to a specific Meta profile. A Meta profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person). Entering "Facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name, but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta information that reveals a particular person purchased prerecorded video content or a subscription to access prerecorded video content on Defendant's Websites (hereinafter, "Private Viewing Information").

5. The information Defendant disclosed (and continues to disclose) to TikTok via the TikTok Pixel includes the customer's cellular telephone number and the subscription to access prerecorded videos or the specific title of prerecorded videos that each of its customers purchased on any one of its Websites. A cellular telephone number or email is required *inter alia* to sign up for a TikTok account, which is set to receive a short code for verification purposes. A TikTok profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person). Entering the cellular telephone number on any search engine or a free reverse lookup site will

return the owner's name. Thus, the cellular telephone number or email used for sign-up identifies a person more precisely than a name, as numerous persons may share the same name, but a cellular telephone number is usually uniquely associated with one and only one person. In the simplest terms, the TikTok Pixel installed by Defendant captures and discloses to TikTok information that reveals a particular person purchased prerecorded video content or a subscription to access prerecorded video content on Defendant's Websites (hereinafter, "Private Viewing Information").

6. Defendant disclosed and continues to disclose its customers' Private Viewing Information to Meta and TikTok without asking for, let alone obtaining, their consent to these practices.

7. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), damages in the amount of $2,500.00, *see id.* § 2710(c).

8. Accordingly, on behalf of themselves and the putative Class members defined below, Plaintiffs bring this Class Action Complaint against Defendant for

intentionally and unlawfully disclosing their and the Putative Class members' Private Viewing Information to Meta.

PARTIES

I. Plaintiff Tracey Damrau

9. Plaintiff Damrau is, and at all times relevant hereto was, a citizen and resident of Suffolk County, New York.

10. Plaintiff Damrau is, and at all times relevant hereto was, a user of Meta and TikTok.

11. Plaintiff Damrau is a consumer of the video products and services offered on Defendant's www.elitelearning.com website. Including on or about July 6, 2024, Plaintiff Damrau purchased an all-access subscription to access prerecorded video material from Defendant's website by requesting and paying for such material, providing her name, email address, and home address for shipment of such material. Defendant completed its sales of goods to Plaintiff Damrau by shipping or delivering the prerecorded video material she purchased to the address she provided in her order. Accordingly, Plaintiff Damrau requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its website.

12. On multiple occasions during the two years preceding the filing of this action, Plaintiff Damrau used her subscription to Defendant's website to request and obtain pre-recorded videos from Defendant.

13. At all times relevant hereto, including when purchasing a subscription to Defendant's website and accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Damrau had a Meta account, a Meta profile, and an FID associated with such profile.

14. At all times relevant hereto, including when purchasing a subscription to Defendant's website and accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Damrau had a TikTok account, a TikTok profile, and her cellular telephone number was associated with such profile.

15. Plaintiff Damrau has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Viewing Information to Meta or TikTok. In fact, Defendant has never even provided Plaintiff Damrau with written notice of its practices of disclosing its customers' Private Viewing Information to third parties such as Meta or TikTok.

16. To illustrate Defendant's disclosure to Meta, when Plaintiff Damrau purchased the "NY Social Work All Access Pass" subscription, the specific title of the subscription, the hashed product code, and her request to "Join Today" to complete her purchase was transmitted to Meta alongside Plaintiff Damrau's FID as seen in the exemplar source code for the Elite Nursing Passport CE Membership below:

Request URL:	https://www.facebook.com/privacy_sandbox/pixel/register/trigger/?id=1565621606813649&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.elitelearning.com%2Fsocial-work%2Fce-membership%2F&rl=https%3A%2F%2Fwww.elitelearning.com%2F&if=false&ts=1729622103109&cd[buttonFeatures]=%7B%22classList%22%3A%22wp-block-button__link%20wp-element-button%22%2C%22destination%22%3A%22https%3A%2F%2Fcheckout.elitelearning.com%2FMAGI%2FCommonForms%2Fshoppingcart%2Fadditems.aspx%3FProductCodes%3D48518-8-US-30-2%26paymentOptionId%3D2183%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Join%20Today%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonText]=Join%20Today&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22Elite%20Social%20Work%20Passport%20CE%20Membership%20-%20Elite%20Learning%20-%20Elite%20Learning%22%7D&cd[parameters]=%5B%5D&sw=3008&sh=1692&v=2.9.173&r=stable&a=tmgoogletagmanager&ec=1&o=4126&fbp=fb.1.1728306477419.455508233633952052&cs_est=true&ler=empty&cdl=API_unavailable&it=1729622096575&coo=false&es=automatic&tm=3&exp=h3&rqm=FGET
Request Method:	GET
Status Code:	200 OK
Remote Address:	157.240.14.35:443
Referrer Policy:	strict-origin-when-cross-origin

17. Once Plaintiff Damrau completed her purchase, the "purchase" event code was sent to Meta alongside Plaintiff Damrau's FID within the same session as the specific title of the prerecorded video material or subscription, product code, and her request to join.

18. Prior to and at the time she purchased prerecorded video material from Defendant, Defendant did not notify Plaintiff Damrau that it would disclose the Private Viewing Information of its customers generally or that of Plaintiff Damrau

in particular, and Plaintiff Damrau has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Viewing Information to third parties. Plaintiff Damrau has never been provided any written notice that Defendant sells, rents, licenses, exchanges, or otherwise discloses its customers' Private Viewing Information, or any means of opting out of such disclosures of her Private Viewing Information.

19. Because Defendant disclosed Plaintiff Damrau's Private Viewing Information (including her FID, phone number unique identifiers, and her purchase of a subscription to access prerecorded video material to Defendant's website) to third parties during the applicable statutory period, Defendant violated Plaintiff Damrau's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

II. Plaintiff Danielle Oshea

20. Plaintiff Oshea is, and at all times relevant hereto was, a citizen and resident of Suffolk County, New York.

21. Plaintiff Oshea is, and at all times relevant hereto was, a user of TikTok.

22. Plaintiff Oshea is a consumer of the video products and services offered on Defendant's www.elitelearning.com website. Including on or about August 22, 2024 and August 28, 2024, Plaintiff Oshea purchased prerecorded video content from Defendant's website by requesting and paying for such material, providing her

name, email address, phone number, and home address for shipment of such material. Defendant completed its sales of goods to Plaintiff Oshea by shipping or delivering the prerecorded video material she purchased to the address she provided in her order. Accordingly, Plaintiff Oshea requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its website.

23. At all times relevant hereto, including when purchasing prerecorded video material provided on Defendant's website, Plaintiff Oshea had a TikTok account and profile and her phone number was associated with such profile.

24. Plaintiff Oshea has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Viewing Information to TikTok. In fact, Defendant has never even provided Plaintiff Oshea with written notice of its practices of disclosing its customers' Private Viewing Information to third parties such as TikTok.

25. To illustrate Defendant's disclosure to TikTok, when Plaintiff Oshea purchased prerecorded video content including the "Managing Professional Boundaries" course, the specific title of the prerecorded video, the hashed product code, and her request to "Join Today" to complete her purchase was transmitted to TikTok during the single continuous session involving her purchase.

26. During Step Two of the registration process for Plaintiff Oshea's purchase of the "Managing Professional Boundaries" course, Defendant's website

specifically required that Plaintiff Oshea provide her phone number, and as she provided her cellular telephone number, the EnrichAM event[1] code was auto-triggered for TikTok to collect Plaintiff Oshea's un-hashed cellular telephone number and then TikTok transmitted her number in hashed value via the TikTok Pixel as seen in the exemplar below:

27. After this information was transmitted, a "Complete Payment" event code was then transmitted from Defendant's website to TikTok via the TikTok Pixel when Plaintiff Oshea submitted her order.

[1] EnrichAM is a Tiktok event code that is used for Enhanced Data Postback that collects more specific information unless a user expressly and separately opts out of its auto collection. *See* TikTok, Enhance Data Postback with the TikTok Pixel, TikTok Bus. Help Ctr., https://ads.tiktok.com/help/article/enhance-data-postback-with-the-tiktok-pixel.

28. At all times relevant hereto, when Plaintiff Oshea purchased prerecorded video content on Defendant's website, TikTok used Plaintiff Oshea's "contact details," as transmitted by Defendant's installation of the TikTok Pixel, to match her purchase and interactions on Defendant's website to her TikTok profile.

29. Prior to and at the time she purchased prerecorded video material from Defendant, Defendant did not notify Plaintiff Oshea that it would disclose the Private Viewing Information of its customers generally or that of Plaintiff Oshea in particular, and Plaintiff Oshea has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Viewing Information to third parties. Plaintiff Oshea has never been provided any written notice that Defendant sells, rents, licenses, exchanges, or otherwise discloses its customers' Private Viewing Information, or any means of opting out of such disclosures of her Private Viewing Information.

30. Because Defendant disclosed Plaintiff Oshea's Private Viewing Information (including her phone number, device identifiers, and her purchase of prerecorded video material on Defendant's website) to TikTok during the applicable statutory period, Defendant violated Plaintiff Oshea's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

III. Defendant Colibri Group, Inc.

31. Defendant is a foreign corporation existing under the laws of the State of Delaware with a principal place of business at 338 S. Spring St Louis, MO 63110. Defendant operates and maintains a portfolio of company and brand Websites, including www.elitelearning.com, www.homeceuconnection.com, www.colibrirealestate.com, www.mckissock.com, and www.fhea.com, where it sells subscriptions to access prerecorded video content and individually priced prerecorded video content from various industries, including nursing, healthcare, home inspection, engineering, appraisal, social work, occupational therapy, pharmacy, counseling, and other fields.

32. Defendant is the parent company governing several companies and brands that collectively comprise the Colibri Group portfolio including Colibri Healthcare, LLC f/k/a Elite Professional Education LLC; Colibri Real Estate, LLC; McKissock, LLC, and Fitzgerald Health Education Associates, LLC.

JURISDICTION AND VENUE

33. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

34. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in St. Louis, MO, within this judicial District.

VIDEO PRIVACY PROTECTION ACT

35. The VPPA prohibits companies (like Defendant) from knowingly disclosing to third parties (like Meta and TikTok) information that personally identifies consumers (like Plaintiffs) as having requested or obtained a subscription to prerecorded video content or a specific video(s) or other audio-visual materials.

36. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4). It defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

37. Leading up to the VPPA's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by

disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

38. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, the personal nature of such information, and the need to protect it from disclosure, is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id*.

39. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a more recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st

Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[2]

40. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[3]

41. In this case, however, Defendant deprived Plaintiff and numerous other similarly situated persons of that right by systematically (and surreptitiously) disclosing their Private Viewing Information to Meta, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

[2] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury.

[3] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, franken.senate.gov (Jan. 31, 2012).

42. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[4]

43. Over two decades later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a 26 billion dollar per year online advertising industry in the United States.[5]

44. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[6]

[4] Transcript, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[5] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), available at https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[6] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

45. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[7]

46. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[8]

47. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[9]

48. Recognizing the severe threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking

---

[7] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), available at http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/ .

[8] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), available at https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html#:~:text=It's%20called%20the%20Acxiom%20Corporation,to%20know%20much%2C%20much%20more.

[9] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. On Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) available at https://www.commerce.senate.gov/services/files/3bb94703-5ac8-4157-a97b-%20a658c3c3061c.

information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[10]

49. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like Colibri share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[11]

50. Disclosures like Defendant's are particularly dangerous to the elderly. "Older Americans are perfect telemarketing customers, analysts say, because they

---

[10] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), available at https://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

[11] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.

are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide."[12]

51. The FTC notes that "[t]he elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[13]

52. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like Defendant's are particularly troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[14]

53. Defendant is not alone in violating its customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

---

[12] *Id*.

[13] Prepared Statement of the FTC on "Fraud Against Seniors" before the Special Committee on Aging, United States Senate (August 10, 2000).

[14] *Id*.

II. Consumers Place Monetary Value on Their Privacy and Consider Privacy Practices When Making Purchases

54. As the data aggregation industry has grown, so has consumer concerns regarding personal information.

55. A survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do protect their privacy online.[15] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[16]

56. Thus, as consumer privacy concerns grow, consumers increasingly incorporate privacy concerns and values into their purchasing decisions, and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[17]

---

[15] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

[16] *Id*.

[17] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), available at https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

57. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[18]

58. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[19] As such, where a business offers customers a product or service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a product or service of less value than the product or service paid for.

III. Defendant Uses Tracking Technology to Systematically Disclose its Customers' Private Viewing Information to Third Parties

59. As alleged below, when a consumer requests or obtains a specific prerecorded video or subscription from one of Defendant's Websites, the tracking technology that Defendant intentionally installed on its Websites transmits the fact

[18] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on Monetizing Privacy* (Feb. 27, 2012), available at https://www.enisa.europa.eu/publications/monetising-privacy.

[19] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

that a consumer purchased a prerecorded video or subscription to video materials or services alongside his or her FID or other personally-identifying information to Meta and TikTok, without the customer's consent and in clear violation of the VPPA.

A. The Meta Pixel

60. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta".[20] Meta is now the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

61. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to monitor and track the actions taken by visitors to their websites and to report them back to Meta. This allows companies like Defendant to build detailed profiles about their customers and to serve them with highly targeted advertising.

62. The Meta Pixel installed on a company's website allows Meta to "match [] website visitors to their respective Facebook User accounts."[21] This is because Meta has assigned to each of its users an "FID" number – a unique and

[20] *See* Facebook, "Company Info," available at https://about.fb.com/company-info./.

[21] Meta, "Get Started – Meta Pixel," available at https://developers.facebook.com/docs/meta-pixel/get-started/.

persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[22] – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor.

63. As Meta's developer's guide explains, installing the Meta Pixel on a website allows Meta to track actions that users with Meta accounts take on the site. Meta states that "Examples of [these] actions include adding an item to their shopping cart or making a purchase."[23]

64. Meta's Business Tools Terms govern the use of Meta's Business Tools, including the Meta Pixel.[24]

65. Meta's Business Tools Terms state that website operators may use Meta's Business Tools, including the Meta Pixel, to transmit the "Contact Information" and "Event Data" of their website visitors to Meta.

[22] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

[23] Meta, "About Meta Pixel," available at https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[24] Meta, "Meta Business Tools Terms," available at https://www.facebook.com/legal/technology_terms.

66. Meta's Business Tools Terms define "Contact Information" as "information that personally identifies individuals, such as names, email addresses, and phone numbers . . . ."[25]

67. Meta's Business Tools Terms state: "You instruct us to process the Contact Information solely to match the Contact Information against user IDs [e.g., FIDs] ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[26]

68. The Business Tools Terms define "Event Data" as, *inter alia*, "information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products."[27]

69. Website operators use the Meta Pixel to send information about visitors to their websites to Meta. Every transmission to Meta accomplished through the Meta Pixel includes at least two elements: (1) the website visitor's FID and (2) the URL of the webpage triggering the transmission.

[25] *Id*.

[26] *Id*.

[27] *Id*.

70. Depending on the configuration of the Meta Pixel, the website may also send Event Data to Meta. Defendant has configured the Meta Pixel on its Website to send Event Data to Meta.

71. When website operators make transmissions to Meta through the Meta Pixel, none of the following categories of information are hashed or encrypted: the visitor's FID, the URL of the website, or the Event Data.

72. Every website operator installing the Meta Pixel must agree to the Meta Business Tools Terms.[28]

73. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

74. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

75. Simply put, if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the

[28] *See id.*

information it transmits) are then able to "track [] the people and type of actions they take,"[29] including, as relevant here, the subscription to access prerecorded video material or the specific prerecorded video material that they purchase on any one of Defendant's website.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the Private Viewing Information of its Customers to Meta

76. Defendant sells a wide variety of subscriptions and prerecorded video materials on its Websites, including continuing education courses, on-demand licensing courses, and other prerecorded videos.

77. Defendant maintains control over and governs the Websites by requiring that each website follow the same uniform policies and identify itself as a Colibri Group website.

78. To purchase prerecorded video material or a subscription to access prerecorded video material from any one of Defendant's Websites, a person must provide at least his or her name, email address, billing address, and credit or debit card (or other form of payment) information.

79. During the purchase process on any one of Defendant's Websites, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to

[29] Meta, "Retargeting: How to Advertise to Existing Customers with Ads on Facebook," available at https://www.facebook.com/business/goals/retargeting?checkpoint_src=any.

disclose to Meta the unencrypted FID of the person who made the purchase and the subscription title or specific title of video material that the person purchased (as well as the URL where such video material is available for purchase).

80. In order to take advantage of the targeted advertising and other informational and analytical services offered by Meta, Defendant intentionally programmed its Websites (by following step-by-step instructions from Meta's website) to include the Meta Pixel code, which systematically transmits to Meta the FID of each person with a Meta account who purchases prerecorded video material on any one of Defendant's Websites, along with the subscription or the specific title of the prerecorded video material that the person purchased.

81. With only a person's FID and the subscription purchase or the title of the prerecorded video material (or URL where such material is available for purchase) that the person purchased from Defendant on any one of its Websites—all of which Defendant knowingly and systematically provides to Meta—any ordinary person could learn the identity of the person to whom the FID corresponds and the subscription or the title of the specific prerecorded video material that the person purchased (and thus requested and obtained). This can be accomplished simply by accessing the URL www.facebook.com/ and inserting the person's FID.

82. Defendant's practice of disclosing the Private Viewing Information of its customers to Meta continued unabated for the duration of the two-year period

preceding the filing of this action. At all times relevant hereto, whenever Plaintiff or any other person purchased a subscription to access prerecorded video material or prerecorded video material from Defendant on any one of its Websites, Defendant disclosed to Meta (*inter alia*) the subscription or the specific title of the video material that was purchased (including the URL where such material is available for purchase), along with the FID of the person who purchased it (which, as discussed above, uniquely identified the person).

83. At all times relevant hereto, Defendant knew the Meta Pixel was disclosing its customers' Private Viewing Information to Meta.

84. Although Defendant could easily have programmed its website so that none of its customers' Private Viewing Information is disclosed to Meta, Defendant instead chose to program its Websites so that all of its customers' Private Viewing Information is disclosed to Meta.

85. Before transmitting its customers' Private Viewing Information to Meta, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

86. By intentionally disclosing to Meta Plaintiff's and its other customers' FIDs together with the subscription purchase or the specific video material that they each purchased, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

C. The TikTok Pixel

87. In September 2016, ByteDance launched a short-form video content platform, which is now known as "TikTok". TikTok is now the leading destination for short-form mobile videos.[30] To create a TikTok account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

88. The TikTok Pixel, first introduced in 2018 is a unique piece of code that can be placed on websites to share website events with TikTok, to measure traffic and ad campaign performance on the website, and to optimize ad campaigns for finding new customers. This allows companies like Defendant to build detailed profiles about their customers and to serve them with highly targeted advertising.

89. Websites, like Defendant's, can transmit through the TikTok Pixel the following information: device platform, webpage URLs viewed, session ID, anonymous user ID, browser information, event codes, currency, email addresses, and phone numbers.

90. Additionally, the TikTok Pixel installed on a company's website allows the company to share its customers' Contact Details – name, email address, and or phone number – with TikTok, for matching purposes.[31] This is because

[30] TikTok, About, https://www.tiktok.com/about?lang=en (last visited Oct. 22, 2024).
[31] TikTok Ads, Product Policy, TikTok, https://ads.tiktok.com/i18n/official/policy/product (last visited Oct. 22, 2024).

TikTok collects Contact Information during a person's sign up – such as first and last name, and phone number – which TikTok then assigns a unique and persistent identifier. The TikTok identifier does not prevent TikTok or anyone else from discovering a person's name by simply looking it up based on their phone number, however. The phone number is still connected to the TikTok account, and the transmissions made from a company's website to TikTok via the TikTok Pixel during the user's continuous session are accompanied by, *inter alia*, the phone number of the website's visitor. Moreover, the TikTok Pixel can follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

91. TikTok has used the TikTok Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all its users' interactions with any of the hundreds of thousands of websites across the Internet on which the TikTok Pixel is installed. TikTok then monetizes its database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

92. Simply put, if a company chooses to install the TikTok Pixel on its website, both the company who installed it and TikTok (the recipient of the information it transmits) are then able to track the user's interactions with that

particular webpage including, as relevant here, the subscription to access prerecorded video material or the specific prerecorded video material that they purchase on any one of Defendant's website.

D. Defendant Knowingly Uses the TikTok Pixel to Transmit the Private Viewing Information of its Customers to TikTok

93. Similar to the Meta Pixel, during the purchase process on any one of Defendant's Websites, Defendant uses – and has used at all times relevant hereto – the TikTok Pixel to disclose to TikTok the device platform, webpage URLs viewed, session ID, anonymous user ID, browser information, event codes, currency, and phone number of the person who made the purchase and the subscription title or specific title of video material that the person purchased (as well as the URL where such video material is available for purchase).

94. In order to take advantage of the targeted advertising and other informational and analytical services offered by TikTok, Defendant intentionally programmed its Websites (by following step-by-step instructions from TikTok's website) to include the TikTok Pixel code, which systematically transmits to TikTok personally identifiable information (a person's cell phone number and other unique device information) of each person with a TikTok account who purchases prerecorded video material or a subscription from any one of Defendant's Websites, along with the subscription or the specific title of the prerecorded video material that the person purchased.

95. With only a person's cell phone number and the subscription purchase or the title of the prerecorded video material (or URL where such material is available for purchase) that the person purchased from Defendant on any one of its Websites—all of which Defendant knowingly and systematically provides to TikTok— TikTok is able to "match" an off-TikTok user with his or her TikTok account with that person's registered name, just like any ordinary person could learn the identity of the person to whom the cell phone number corresponds by simply, among other ways, doing a free online reverse lookup. Once looked up, an ordinary person has a person's identity and the subscription or the title of the specific prerecorded video material that the person purchased (and thus requested and obtained).

96. Defendant's practice of disclosing the Private Viewing Information of its customers to TikTok continued unabated for the duration of the two-year period preceding the filing of this action. At all times relevant hereto, whenever Plaintiffs or any other person purchased a subscription to access prerecorded video material or prerecorded video material from Defendant on any one of its Websites, Defendant disclosed to TikTok (*inter alia*) the subscription or the specific title of the video material that was purchased (including the URL where such material is available for purchase), along with the FID of the person who purchased it (which, as discussed above, uniquely identified the person).

97. At all times relevant hereto, Defendant knew the TikTok Pixel was disclosing its customers' Private Viewing Information to TikTok.

98. Although Defendant could easily have programmed its website so that none of its customers' Private Viewing Information is disclosed to TikTok, Defendant instead chose to program its Websites so that all of its customers' Private Viewing Information is disclosed to TikTok.

99. Before transmitting its customers' Private Viewing Information to TikTok, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

100. By intentionally disclosing to TikTok Plaintiffs' and its other customers' phone numbers together with the subscription purchase or the specific video material that they each purchased, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

101. Plaintiff Damrau seeks to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, purchased prerecorded video material or a subscription to access prerecorded video material or services from any one of Defendant's portfolio of Websites while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

102. Plaintiff Damrau and Plaintiff Oshea seek to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, purchased prerecorded video material or a subscription to access prerecorded video material or services from Defendant's www.elitelearning.com or www.colibrirealestate.com websites while maintaining an account with TikTok, Inc.

103. Members of the Classes are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Classes number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Members of the Classes may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

104. Common questions of law and fact exist for all members of the Classes and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to (a) whether Defendant embedded tracking pixels on its Websites that monitor and track actions taken by visitors to the Websites; (b) whether Defendant reports the actions and information of visitors to third parties; (c) whether Defendant knowingly disclosed Plaintiffs' and members of the Classes' Private Viewing Information to third parties; (d) whether Defendant's conduct violates the Video Privacy Protection Act,

18 U.S.C. § 2710; and (e) whether Plaintiffs and members of the Classes are entitled to a statutory damage award of $2,500, as provided by the VPPA.

105. The named Plaintiffs' claims are typical of the claims of members of the Classes in that the Defendant's conduct toward the putative class is the same. That is, Defendant embedded tracking technologies on its Websites to monitor and track actions taken by consumers on its Websites and report this to third parties. Further, the named Plaintiffs and members of the Classes suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Private Purchase Information to third parties.

106. Plaintiffs are adequate representatives of the Classes because they are interested in the litigation; their interests do not conflict with those of the Class members they seek to represent; they have retained competent counsel experienced in prosecuting class actions; and they intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of all members of the Classes.

107. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual member of the Classes may lack the resources to undergo the burden and expense of individual

prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication of the common questions of law and fact, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION
Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

108. Plaintiffs repeat the allegations asserted in the preceding paragraphs as if fully set forth herein.

109. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

110. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar

audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of selling and delivering prerecorded video materials and subscriptions to access prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

111. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiffs and members of the Classes are each a "consumer" within the meaning of the VPPA because they each purchased prerecorded video material or a subscription to access prerecorded video material or services from any one of Defendant's Websites that was sold and delivered to them by Defendant.

112. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The Private Viewing Information that Defendant transmitted to Meta constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because it identified Plaintiffs and members of the Classes to third parties as an individual who purchased, and thus "requested or obtained," a subscription to access

prerecorded video material or specific prerecorded video material from one of Defendant's Websites.

113. Defendant knowingly disclosed Plaintiffs' and members of the Classes' Private Viewing Information to Meta via the Meta Pixel technology because Defendant intentionally installed and programmed the Meta Pixel code on its Websites, knowing that such code would transmit the subscription or prerecorded video material purchased by its consumers and the purchasers' unique identifiers (including FIDs).

114. Defendant knowingly disclosed Plaintiffs' and members of the Classes' Private Viewing Information to TikTok via the TikTok Pixel technology because Defendant intentionally installed and programmed the TikTok Pixel code on its www.elitelearning.com and www.colibrirealestate.com websites, knowing that such code would transmit the subscription or prerecorded video material purchased by its consumers and the purchasers' cellular telephone number, browser and device information.

115. Defendant failed to obtain informed written consent from Plaintiffs or members of the Classes authorizing it to disclose their Private Viewing Information to any third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who purchased prerecorded video material or a subscription to access prerecorded video material

or services on its Websites (including Plaintiffs or members of the Classes) informed, written consent that was given in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

116. By disclosing Plaintiffs' and members of the Classes' Private Viewing Information, Defendant violated their statutorily protected right to privacy in their Private Viewing Information.

117. Consequently, Defendant is liable to Plaintiffs and members of the Classes for damages in the statutorily set sum of $2,500. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek a judgment against Defendant Colibri Group, Inc. as follows:

a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Classes and Plaintiffs' attorneys as Class Counsel to represent the Classes;

b) For an order declaring that Defendant's conduct as described herein violated the VPPA;

c) For an order finding in favor of Plaintiffs and the Classes and against Defendant on all counts asserted herein;

d) For an award of $2,500.00 to Plaintiffs and each member of the Classes, as provided by 18 U.S.C. § 2710(c);

e) For an order permanently enjoining Defendant from disclosing the Private Viewing Information of its purchasers and subscribers to third parties in violation of the VPPA;

f) For prejudgment interest on all amounts awarded; and

g) For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiffs and the Classes under Rule 23 and 18 U.S.C. § 2710(c).

Respectfully submitted,

Dated: October 25, 2024

HEDIN LLP

/s/ *Elliot O. Jackson*
Elliot O. Jackson
MO Reg. No. #1034536(FL)
1395 Brickell Ave., Suite 610
Miami, Florida 33131-3302
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
ejackson@hedinllp.com

Julie E. Holt*
1395 Brickell Ave., Suite 610
Miami, Florida 33131-3302
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
jholt@hedinllp.com

Counsel for Plaintiffs and Putative Class

**Application for admission Pro Hac Vice forthcoming*